



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,571	01/12/2004	Kensaku Yamaguchi	247558US2RD	8239
22850 7590 09/17/2008 OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			EXAMINER TURCHEN, JAMES R	
			ART UNIT	PAPER NUMBER
			2139	
			NOTIFICATION DATE	DELIVERY MODE
			09/17/2008	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com  
oblonpat@oblon.com  
jgardner@oblon.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/754,571	<b>Applicant(s)</b> YAMAGUCHI ET AL.	
	<b>Examiner</b> JAMES TURCHEN	<b>Art Unit</b> 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 18 June 2008.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## DETAILED ACTION

Claims 1-8 are pending.

### ***Response to Arguments***

Applicant's arguments filed 06/18/2008 have been fully considered but they are not persuasive.

Regarding claims 1 and 5:

Examiner respectfully disagrees with applicant regarding the arguments to claims 1 and 5. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the encryption key is not stored in the cache memory) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claim specifically states that each cache line having a secret protection attribute holding section for storing an actual encryption key, but does not state that the key is located in a physical location in the cache memory. Hashimoto discloses a secret protection attribute holding section in the key value table [*paragraphs 127 and 102*].

Regarding claims 2-4 and 6-8:

Examiner respectfully disagrees with applicant regarding the arguments to claims 2, 3, 6 and 7. It is true that Hashimoto compares the identifiers and Hashimoto discloses the comparing of keys via the comparing of the identifiers. The identifiers are used to point to individual keys, therefore if the identifiers are different, then the keys

Art Unit: 2139

themselves must also be different [paragraph 127]. Paragraph 102 discloses that the data key identifier is used to find the key to encrypt the data that is being sent to memory.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Hashimoto et al. (JP02002232417A; hereafter Hashimoto).

Regarding claims 1 and 5:

Hashimoto discloses tamper resistant microprocessor and data access control method that executes a plurality of programs in parallel under a multi-task programming environment, comprising:

a decryption unit configured to read out an execution code or data of one of a plurality of encrypted programs and decrypt the execution code or data by using a prescribed encryption key corresponding to the read-out encrypted program, according to a decryption request from a cache memory control unit [paragraph 16, *1st decoding means decrypts an instruction key read by a 1st reading means (a cache read) using a secret key; paragraph 19, cryptographic stage acquires decode key corresponding from 1st table in reading and writing with cache memory and external memory based on tag values shown from cache memory*];

a cache memory configured to store the execution code or data decrypted by the decryption unit into one of cache lines provided in the cache memory, each cache line having a secret protection attribute holding section for storing an actual encryption key used in decrypting the execution code or data, the execution code or data stored in the cache memory remaining even after each program terminates [*paragraphs 43-45 the cache tag is performing access control of the confidential information of the process on cache memory; the encryption key at the time of certain cache data is determined by the encryption attribute tag*]; and

the cache memory control unit configured to process a reading request for the execution code or data to be acquired from the decryption unit or the cache memory such that, if the execution code or data exists in the cache memory and the actual encryption key stored in the secret protection attribute holding section of a cache line that stores the existent execution code or data is identical with the prescribed key corresponding to a program that issues the reading request, the execution code or data in the cache memory is read out, and if the execution code or data does not exist in the cache memory or the actual encryption key is not identical with the prescribed key, the execution code or data is read out from an external memory device [*paragraph 50, if the cache tag consists of an attribute of an address and others is outputted and a tag is in agreement, a command will be outputted to the processor; paragraph 72, when cache does not hit, address information is sent to the command decoding processing part, reads and decrypts an enciphered program from external memory*].

Regarding claims 2 and 6:

Art Unit: 2139

Hashimoto discloses the tamper resistant microprocessor and data access control method of claims 1 and 4, further comprising:

a key value register configured to store the prescribed encryption key, which is updated at an occasion of executing each encrypted program [*paragraphs 80-82, the decrypted cache line to instruction cache read is stored in an entry with an instruction cache, the tag containing an effective key identifier will be written in the tag area*];

wherein the cache memory control unit judges whether the actual encryption key stored in the secret protection attribute holding section of a cache line that stores the existent execution code or data is identical with the prescribed key stored in the key value register [*paragraphs 80-82, the cache is checked for a dirty bit which would indicate that the cache line needs to be replaced*].

Regarding claims 3 and 7:

Hashimoto discloses the tamper resistant microprocessor and data access control method of claims 2 and 6, wherein the cache memory stores data decrypted by the decryption unit, and the cache memory control unit writes a processing result of the data into the cache memory, while storing the prescribed encryption key stored in the key value register into the secret protection attribute holding section of a cache line for the data [*paragraph 80, the decrypted cache line to instruction cache read is stored in an entry with an instruction cache, the tag containing an effective key identifier will be written in the tag area*].

Regarding claims 4 and 8:

Hashimoto discloses the tamper resistant microprocessor and data access control method of claims 1 and 5, wherein the cache memory stores data decrypted by the decryption unit, and the cache memory control unit encrypts a processing result of the data by using the actual encryption key stored in the secret protection attribute holding section of a cache line for the data, and writes encrypted data into the external memory device [*paragraph 82, data is returned to main memory by external memory (enciphered with a common key)*].

### **Conclusion**

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES TURCHEN whose telephone number is (571)270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

Art Unit: 2139

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571)272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

/Kristine Kincaid/  
Supervisory Patent Examiner, Art Unit 2139